

INFORMATION SYSTEMS SECURITY COMPLIANCE IN E-GOVERNMENT

Stephen Smith

Senior Project Officer, Federated Information Exchange
Office of the Government Chief Information Officer
Department of Commerce
Level 21, McKell Building, 2-24 Rawson Place, Sydney, NSW 2000, Australia
Stephen.Smith@commerce.nsw.gov.au

Donald Winchester

Research Fellow, Security, E-Business, Assurance Research (SEAR) Group
School of Information Systems, Technology and Management
Australia School of Business
University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
d.winchester@unsw.edu.au

Rodger Jamieson

Visiting Professor of Information Systems
School of Information Systems, Technology and Management
Australia School of Business
University of New South Wales
ANZAC Parade, Kensington, Sydney, NSW 2052, Australia.
r.jamieson@unsw.edu.au

Hung T Nguyen

Associate Dean, Research and Development
Faculty of Engineering and Information Technology
University of Technology, Sydney
Broadway, NSW 2007, Australia
Hung.Nguyen@uts.edu.au

Abstract

The aim of this research paper is the development of a Fuzzy Logic model framed on Activity Theory to predict and benchmark compliance of Government agencies activities, with information systems security (ISS) standard, AS17799 (2006). The ISS standard has 10 main categories and 127 controls for which survey questions were asked in an online process. This project is a longitudinal study that commenced in 2002. The questions for the Fuzzy Logic project were piloted in August 2002, followed by three annual surveys from November 2002. The paper describes the development of an enhanced Fuzzy Logic model using Activity Theory. The results from the Fuzzy Logic model helped to focus attention and monitor the progress of agencies that appear unlikely to reach ISS compliance. The main contribution of this study is the simplification of a complex system guided by Activity Theory using a fuzzy logic tool for analysis of a large number of inputs across a large number of agencies. A practical contribution to the New South Wales Government was that the Fuzzy Logic tool removed the complexity in computation, saved time and resources. Our approach using Fuzzy Logic also permits input from expert's embracing an organisations human capital.

Keywords: Information Systems (IS) Security, e-Government, Fuzzy Logic, Dynamic Systems.

1 INTRODUCTION

An important aspect of modern government business is the development of e-Government systems. “E-Government is the use of information and communication technologies (ICT) to improve the activities of public sector organisations” (Heeks 2002, p.3). Consequently many governments are endeavouring to develop policies and procedures to improve security (Frank 2003). From the public’s perspective, government is seen as one entity; hence a security problem within one agency is reflected across the whole of government process. In a domain where the maintenance of public confidence is seen as paramount, the process of improving security across government is viewed as critical. Governance standards and frameworks like: Australia Standard, AS17799:2006 (hereafter AS17799); British Standard, BS7799; or International Organisation for Standards (ISO) / International Electrotechnical Commission (IEC) (e.g., ISO/IEC 17799:2005, ISO27001:2006), all rely on metrics. The determination of the status of an information systems security against the IS security (ISS) standard, ISO/IEC 17799:2005, or similar or superseded standards within an organisation are of key concern. The fundamental requirements of these standards are the same ISO27001:2006, the International Standard for information security management. It is supported by ISO 17799:2005, that is an International Standard providing best practice guidance on security controls that should be considered for implementation within an organisation.

A key criterion in our study is compliance with the relevant standard, which “is highly regarded as the most-recognised standard for managing information security” (Groves 2003), being Information Security Standard AS17799 within Australian. The AS17799 certification encompasses guidance on physical, personnel and environmental security, addresses technical security of communications links and specifies how information technology (IT) system access, for development and maintenance purposes, is controlled. Determining whether an organisation is, or is on target to be, compliant with, has proven difficult for those tasked with managing the organisation security effort. A valid reason for modeling metrics is to save time and costs, improve accuracy, analyse large amounts of data, and to report or present the output in a meaningful manner.

This paper applies fuzzy logic modeling via activity theory to information systems (IS) security managers’ online survey responses, interviews, and other secondary data sources, across a large number of New South Wales (NSW) State government agencies, in Australia. The fuzzy logic model was developed using an interactive learning approach. The purpose of this model is to rank agencies IS security compliance level into a single list into three arbitrary groups from the most compliant to least compliant classified as: limited or no progress; making slow progress; and making good progress and expect to comply on schedule, based on a fuzzy logic analysis of the survey questions. The fuzzy model allowed the IS security manager’s to determine their agencies progress compared (ranked) to other agencies. Thus agencies with a higher confidence value were deemed on-track agencies while agencies with a lower confidence value were scrutinised more closely as they were making the slowest progress.

The main advantage of Fuzzy Logic analysis was its ability to quickly process the subsequent survey responses and produce a ranked list for management. We report the results involving the development and application of fuzzy logic technology to the process of identifying government agencies at risk of not meeting a mandated deadline for compliance with the IS security standard, AS17799. Using fuzzy logic as a predictive and pattern recognition tool in IS security is well documented in the literature (Baskerville 1993, Clements 1977, Hoffman & Michelman & Clements 1998). The focus of this study is to determine the factors or groups of factors that would assist in producing an improved level of security based on AS17799. Examples of fuzzy logic used in other areas include: detection of medical conditions; seat allocation for airlines; and stock market and foreign exchange prediction tools (Ghosh & Razouqi & Schumacher & Celmins 1998). The rest of the paper is organised as follows. Section 2 provides a literature review of theory used in the study and related theories. In Section 3 we describe the research methodology. Section 4 develops an extended fuzzy logic model of activity theory. Our

discussion of results is in Section 5, and Section 6 discusses implications and limitations. Section 7 concludes and gives future research directions.

2 LITERATURE REVIEW AND THEORY

2.1 Activity Theory - Overview

Russian psychologists Vygotsky, Rubinshtein, Leont'ev and Lurija developed activity theory. This theory is a philosophical framework that allows the study of different forms of human practice. This theory can be observed as a developing process where the individual and social levels are interlaced. Vygotsky introduced the concept artefact-mediated and object-oriented action (Vygotsky 1978).

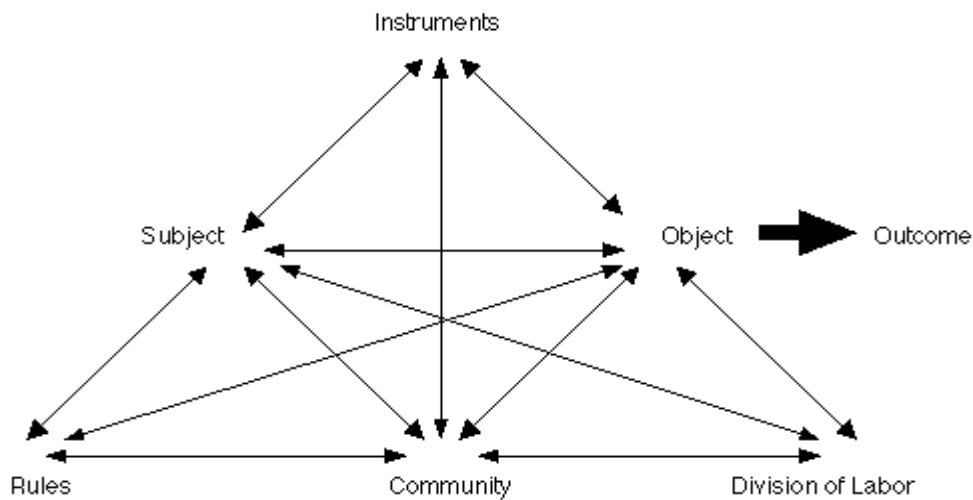


Figure 1. The structure of human activity (Engeström, 1987, p.78).

Leont'ev expanded Vygotsky's model, by introducing human beings and social relations as two mediating forces (Engeström 1998). The aim of the original theories was to "explain cultural practices (e.g., work, school) in the developmental, cultural and historical context in which they occur, by describing them in terms of activities" (Rogers 2001). The backbone of this theory is presented as a hierarchical model of activity, which details different levels, in terms of operations, actions and activities.

Activity theory is an expansive theoretical framework that can be used to detail the structure, development and context of the tasks that can be delivered by a computerised system. This framework proposes the amalgamation of numerous theories and concepts, thus preserving the conceptual integrity of activity theory in terms of design, evaluation and usage. Activity theory is also a social theory designed as a mechanism to understand and explain human activity and interaction. By definition, an activity cannot exist as an isolated entity. Where the subject is an entity engaged in an activity and this activity is directed towards an object, activity theory postulates that the activity mediates interaction between the subject and object (Bannon 1997). Activity theory has been extensively used in IS research by Hasan, Gould and Hyland (2001), Vrazalic (2001) and many other authors. "Recent decades have seen an intensive interaction between psychology and the theory of artificial intelligence. Both psychologists and cognitive scientists have made many attempts to use the apparatus of artificial intelligence and the operational principals of artificial systems in the study of cognition, creativity, and behaviour" (Engeström 1998, p. 348). Activity theory will be used in this particular research, as it appears to fit with views of IS security from this area.

2.2 Activity Theory – Conceptual Model

Figure 2 shows the conceptual model for maintaining security to AS17799 in the e-Government domain (Smith 2006). A review of how to maintain security in e-Government systems is undertaken for security breaches by first analysing the ‘subject’ and ‘object’ involved. Then, describing how this activity is mediated by policies, procedures, technology and the ‘community’ (environment) and finally the ‘division of labour’ within the model illustrated in Figure 2. Figure 2 is linked to Engeström’s model as described in Figure 1. Smith’s (2006) model is specific to information security in the e-Government domain and breaks down the psychological aspects involved in measuring e-Security across the NSW public sector. In essence, the model recognises that several categories (instruments, subject, rules, community, division of labour, and object) are involved in achieving a good level of information security (outcomes).

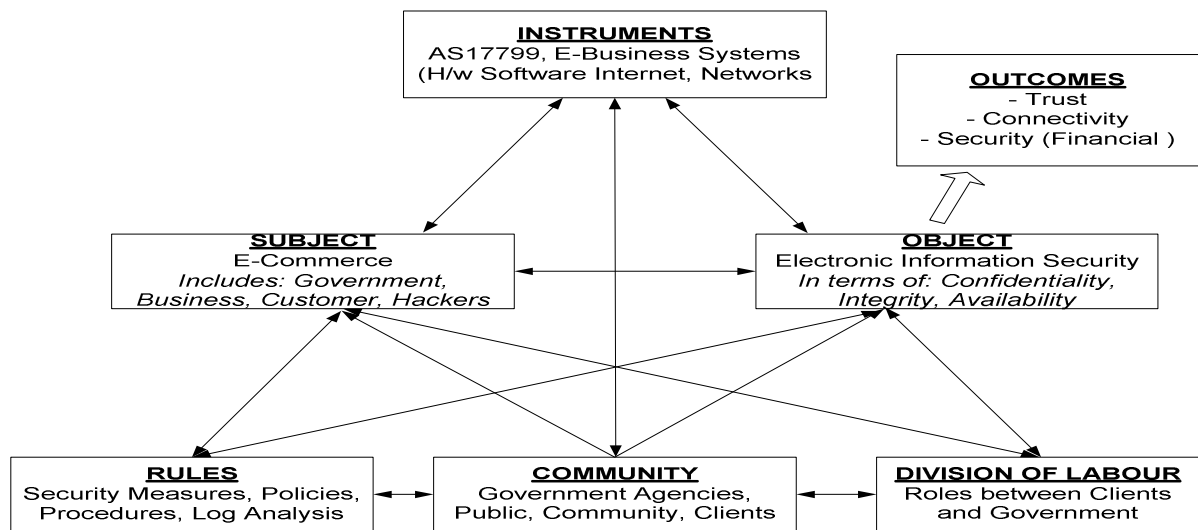


Figure 2. Conceptual Model for Maintaining Security to AS17799 in the e-Government Domain

The instruments node describes the tools used to achieve information security. Examples include: AS17799; e-Business systems (Hardware and Software); Internet; and networks. The object node means electronic information security in this context with respect to confidentiality, integrity and availability. The subject node refers to where the responsibility of the activity rests. In the security model (Figure 2) it is the NSW public service (or more generally, the public service), and participating universities (University of Technology Sydney, University of New South Wales). If the model were in a different context such as, Internet Security across the world, the subject might be CERT (CERT® Coordination Centre). Rules refer to the boundaries governing the activity e.g., security measures; policies; procedures; and log analysis. The community node refers to the social basis of the activity. Examples include: government agencies; business; public; community; and clients. The division of labour node refers to the division of labour within the community’s node. For example, labour is divided based on background discipline and skills. Being specific to the security model (Figure 2) labour could be divided in to a group of programmers, system architects, policy makers and management. A classical organisational structure would represent the division of labour (or labor in the United States) within a government agency.

3 RESEARCH METHODOLOGY

In May 2001, the NSW Government mandated using Circular, C2001-46 (Premiers Circular 2001) that by December 2004 (this was later extended to 2006) all NSW state government agencies would be compliant with Information Security Standard AS17799. As part of that mandate this research study

was instigated to monitor the government agencies progress in achieving the desired compliance by the desired date. The fuzzy logic project began in August 2001 with a pilot, followed by three surveys in November 2001, November 2002 and was completed in November 2004. The fuzzy logic project was part of a larger IS security study which started in the first quarter of 2001 and is ongoing (see Figure 3). The study involved the collection and interpretation of data from three online surveys from 130 (in 2004) government agencies. There were 87 agencies whose data was used in the fuzzy logic analysis. The excluded agencies had exemptions (10) or were budget constrained agencies (33). The ongoing objective of the study is to benchmark and improve the level of security across agencies, and identify and assist agencies that may have a high risk of not achieving an improved level of security. The fuzzy logic study was part of a larger study that started in 2001 and involved online surveys, focus groups, round tables and interviews with key staff (see Figure 3). The Premiers directive, circular, PC2001-46, required the nomination of an IT security contact within each government agency. Each agency was required to complete each survey as it was made available. The on-line surveys were completed by the IT security contact via a secure mechanism and were mandatory to have completed within a specified period of time. Sanctions including informing the relevant minister of failure to participate ensure near 100% compliance to all surveys to date. Each agency received a report of their survey response, which included comparative performance figures.

The study covered organisations ranging from small office's (with less than 20 full-time employees) to organisations with over several thousand staff across many buildings in different localities. The objective of the study was to measure progress towards each agency's compliance with the standard and accordingly the questions in the survey were based on elements of the AS17799. Figure 3 shows the layout of the survey that has been divided into three (3) phases that introduced questions covering nine (out of the 10) categories different of AS17799 in stages to lessen the burden on IS managers of gathering large amounts of secondary data when answering the online survey questions. This was because the time estimated to complete the surveys was kept to approximately 30 minutes. No questions were asked for the fourth category (personnel) as this is covered by NSW or Federal legislation for employment in government environments.

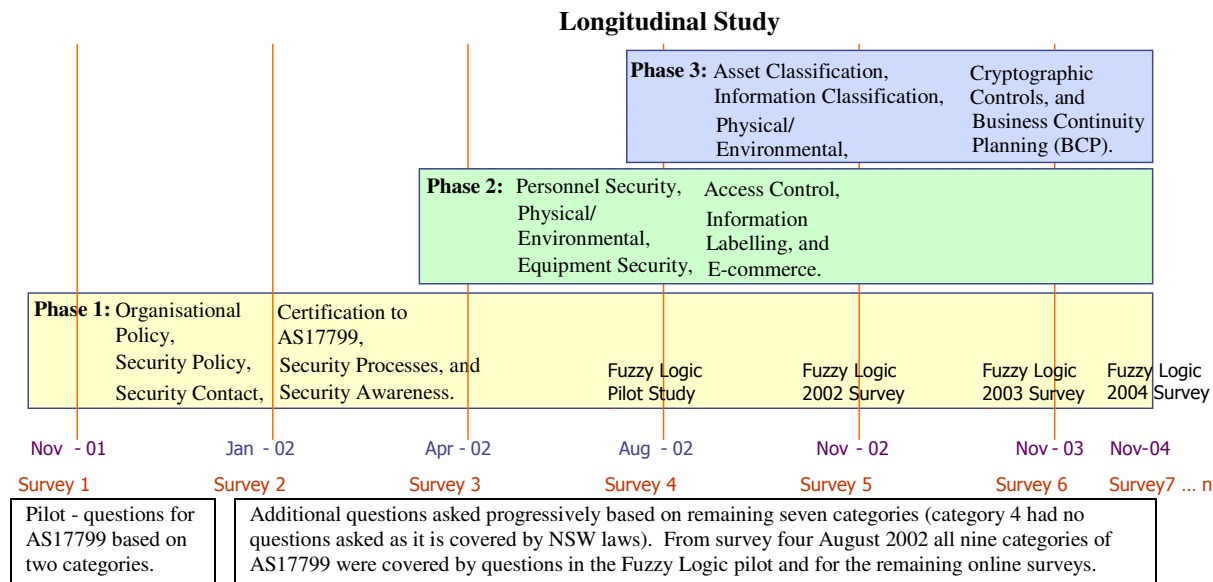


Figure 3. Security Issues Covered by the Surveys.

A fuzzy logic model was developed for the purpose of identifying agency compliance to the Australian Standard, AS17799 (Cox 1994, Halpern 2003, Hung & Nichani 2002, Klir 1999, Nguyen 2006, Zadeh 1983). Fuzzy logic models have previously been used in IS and to evaluate organisational performance from survey responses (Ammar & Moore & Wright 2008, Ammar & Wright 1995,

Ammar & Wright & Selden 2000). After reviewing our survey results collected it was recognised that different elements of the data impacted uniquely on the compliance level to AS17799. Some aspects were more important than others in terms of the overall compliance level of an agency e.g., an agency having a security policy and plan compared to the number of firewalls on the communications networks. This led to the idea of grouping the survey questions in accordance with activity theory using the nine categories of AS17799 as principal variables.

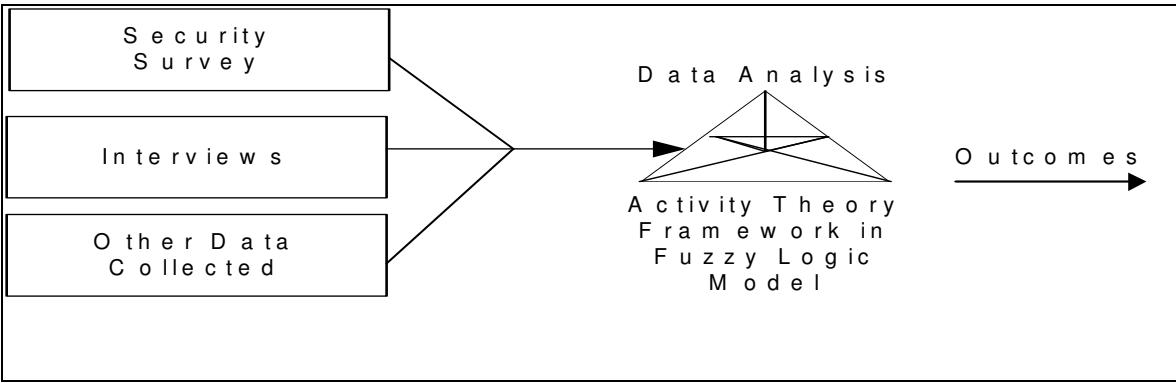


Figure 4. Proposed Model for Identifying an Agencies Compliance Status.

We describe the enhancement of this concept to include activity theory integrated with fuzzy logic to develop a real-world model (Figure 4). This will be achieved by defining structures of activity and relationship among managers, their organisations and security issues. Information system security is the effective implementation of policies to ensure the confidentiality, availability and integrity of information and assets are protected from theft, tampering, manipulation or corruption. Business continuity planning (BCP) is planning to mitigate the adverse effects of an unexpected catastrophe.

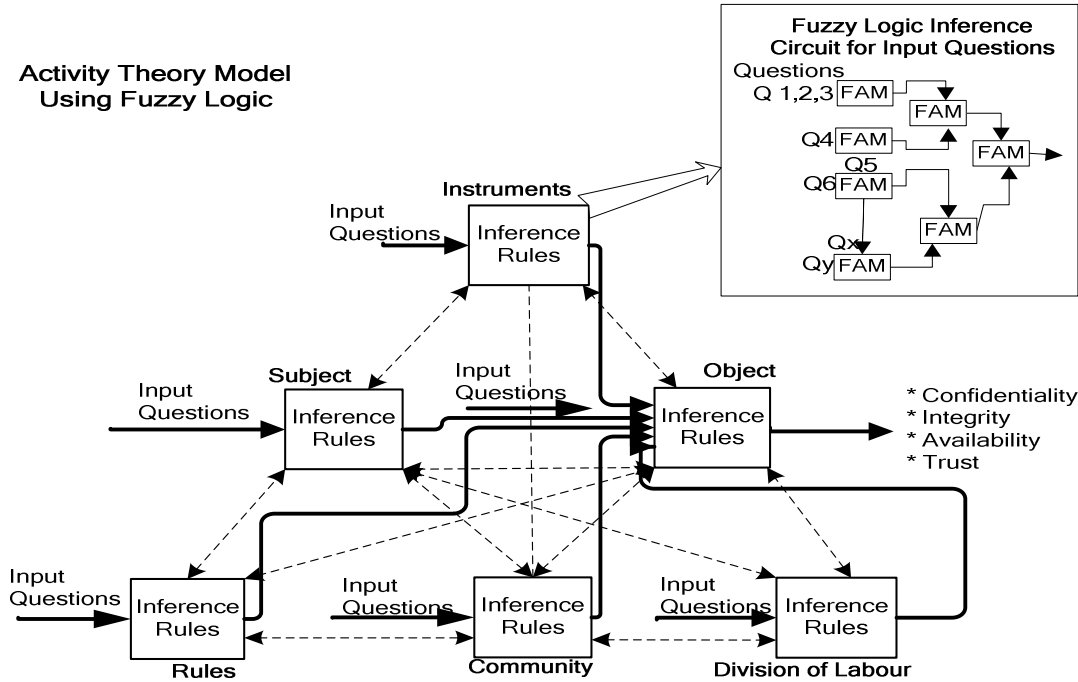


Figure 5. Activity Theory Model Using Fuzzy Logic.

The model developed in Figure 5 was designed to capture an expert's interpretation in order to determine an agency's compliance level. Fuzzy linguistic terms (i.e., positive small, positive medium, positive large) were used as the descriptive language within the model, and fuzzy associative memory (FAM) tables held 'fuzzy' knowledge about each of the survey questions (Q).

The idea behind the process was to find a simple way of measuring an agency's compliance, without the need for a traditional mathematical approach. The first part of the model involves mapping the security survey inputs to linguistic fuzzy terms. This is the fuzzification process and is achieved via a membership function. A uniform triangular membership function was used, other membership functions have not yet been considered for this model.

The next part of the process involved inferring different forms of confidence values from the fuzzy data set. For example, consider the following survey questions:

(A). "How would you rate the level of security across your e-Government system?" Rated (1, 2, 3, 4, or 5), where 1 is low and 5 is high.

(B). "How many significant security incidents have you had in the last 12 months?" Rated (1 – none; 2 – two to five; 3 – six to nine; 4 – 10 to 19; and 5 – more than 20).

In both questions values 1 to 5 are the values saved into the database when a respondent is answering the questions. However, in question (A), a respondent answering a one indicates a low confidence factor, whereas in question (B), a one represents a high confidence factor.

The general nature of the fuzzy approach allows each question to be mapped in such a way so as the output of the fuzzy system represents a consistent confidence factor scaled relative to the other survey questions. In the above example, it would be a matter of reversing the fuzzy associative memory tables for question (B) in order to obtain a reversal of the output confidence factor. More questions that are complicated are also possible where the highest confidence factor is not at the extremities of the input values but perhaps in the middle. In addition, multiple confidence factors (such as two or more highs at different points or perhaps two mediums with no highs) are also possible as well as many other useful mappings. One advantage of implementing it in this fashion is that coding for the confidence mappings is standardised to the fuzzy domain. This means confidence mappings can be flexibly adjusted by an expert without recoding (to validate the results). A major challenge of fuzzy logic systems is that of validating the results. The usual method is to rely on experts to do this and thus, there will be issues related to different opinions given by different experts. We used experts' opinions who were well experienced in artificial intelligence systems, and survey methodologies to aid us validate the model.

Multiple fuzzy associative memory tables are generated at runtime to condense the output of the model down to one value representing a compliance confidence level to the AS17799 standard. The runtime fuzzy tables were based on a standard fuzzy table hard coded in to the system. It was viewed that only the first fuzzy layer required adjustment by an expert. The final fuzzy value was defuzzified using the centre of area (COA) technique providing a confidence value number between 0 and 1.0 indicating the compliance level to AS7799. The survey questions were grouped according to the activity theory model as shown in Figure 2. The model developed and used is shown in Figure 5.

4 EXTENDED FUZZY MODEL OF ACTIVITY THEORY

After some success with the first fuzzy logic the concept of incorporating activity theory to model the social relationships between the different aspects of the Australian security standard seems like it would enable better focus and management of the fuzzy logic. As part of the continual need for development with regards to security, a model mapped directly to the derived Engeström model (as shown in Figure 2) would greatly assist agencies with their process of continual quality improvement. The purpose is to promote an activity within the agency to improve IS security. "Activity theory considers social and cultural properties of the environment to be as objective as the physical and

biological ones, so that activity theory distinguishes between two kinds of objects: physical (material) objects and ideal (mental) objects, present in the subjects mind” (Hasan 1999, p. 48). The interview and survey tool used to measure any successful outcome needs to be attached to some form of measure. The proposal is to model the activity within fuzzy logic model, thus creating a predictive tool for further work in this area. The concept is to take each of the six nodes (rules, community, division of labour, subject, object, and instruments) on the activity theory security maintenance model described in Figure 2, and develop each in to a fuzzy logic as shown in Figure 5. The survey questions are categorised as either being an instrument, subject, rule, community, object, or as a division of labour. The survey results for each category are then fed in to their respective nodes in order to determine an overall compliance level.

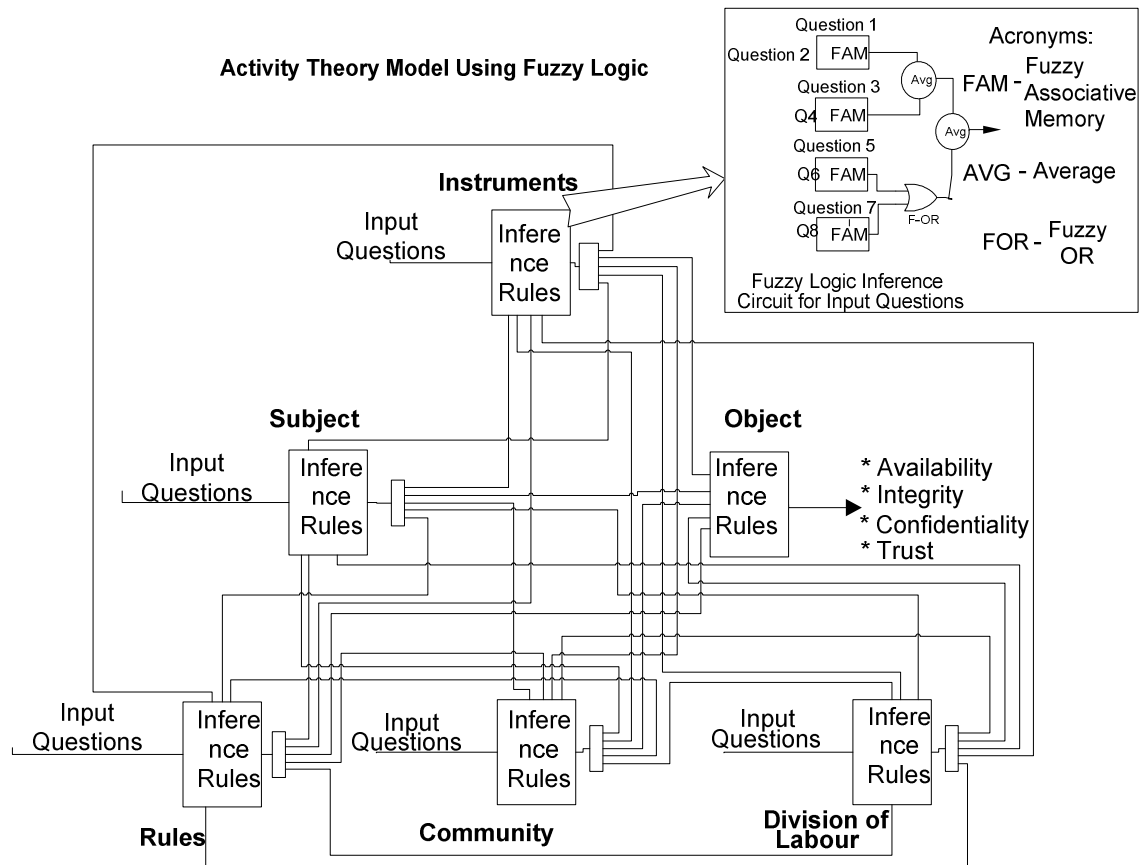


Figure 6. Extended Fuzzy Logic System

An extended fuzzy logic system was also developed and tested. The design shown in Figure 6 is also based on the activity theory model in Figure 2 and considers a set of inference rules based on a fuzzy logic system. Within each inference node fuzzy associated memory (FAM), tables combined with fuzzy logic are constructed in a way that trades two survey questions against each other.

The fuzzy logic circuit was constructed in this trade-off fashion, as we considered a simpler approach by trying to create multi-dimensional lookup tables. In addition, considering two questions together when determining the associative memory values is much easier than trying to evaluate the rules where more than two questions are involved simultaneously (i.e., Fuzzy or (FOR) Average).

In contrast to our previous models, the survey input questions are divided up into the various categories (instruments, subject, object, rules, community, and division of labour). The survey result values are then fed into their respective node associative memory tables and fuzzy logic circuits. Feed back paths are shown in Figure 6, which means that each node can affect each other node according to

Engeström's (Engeström, 1998) psychological model. The advantages and disadvantages of the model illustrated in Figure 6 are:

Advantages:

- Simpler than a neural network model.
- Expert knowledge embedded into lookup tables

Disadvantages:

- Fuzzy logic requires an expert to adjust the lookup tables appropriately (often using a subset of up to 10 principal variables. Our expert used the six nodes as a subset).
- It is more difficult for a fuzzy system to be retrained in the same way as, for example a neural network given changing circumstances. Although it is possible to use self-organising fuzzy logic to retrain the model, it is more complex to develop guaranteed convergence conditions.

As the fuzzy model in Figure 6 proved more successful in tests, we proceeded with the development of a test model based on version 2 of the low level design.

5 DISCUSSION OF RESULTS

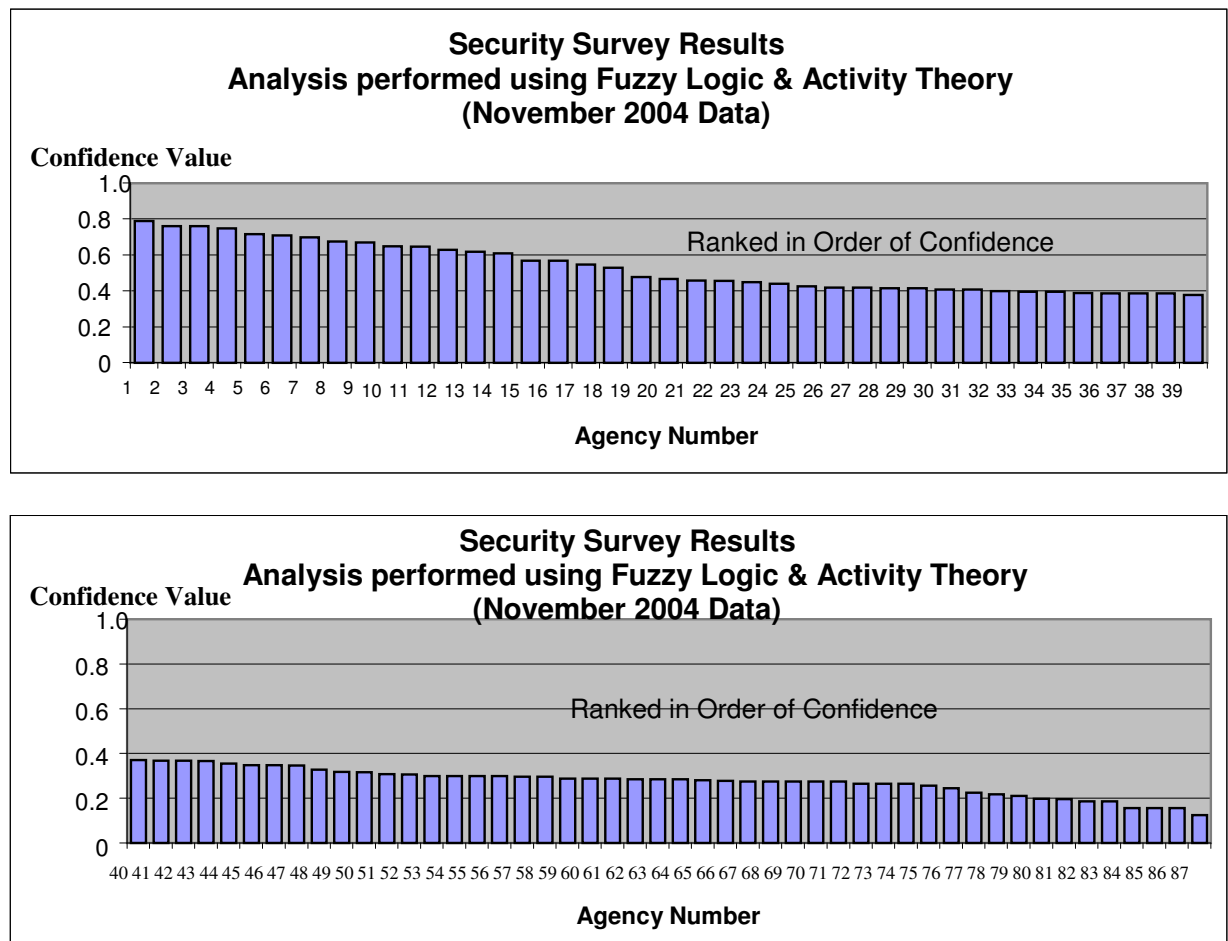


Figure 7. Security Survey FL Results (Both Figures - Agency numbers 1-39 and 40-87).

Figure 7, illustrates the survey results (ranked in order of confidence) of analysis performed using fuzzy logic and activity theory on November 2004 for agencies coded from 1 to 87. The results from using the fuzzy logic model show promise with matching the assessments made by the managers of ISS. The results from the fuzzy logic model allow government agencies to be classified into three

groups - limited or no progress (i.e., confidence values from 0 to 0.3 - an arbitrarily set number); making slow progress (i.e., values from 0.3 to 0.4); and making good progress and expect to comply on schedule (i.e., values from 0.4 to 1). The results in Figure 7 show that agencies from number 1 to 31 were making good progress and were expected to be accredited to AS17799 on schedule. Agencies with numbers from 32 to 52 (21 agencies) were making slow progress while agencies coded with numbers from 53 to 87 (35 agencies) were making limited or no progress. The results from running the fuzzy logic model were used to help select the sample of organisations, from which key personnel (namely the ISS manager) would be interviewed in the next stage of this research program.

Once the agencies were identified, an activity theory framework was proposed to identify and facilitate activities with the key staff to improve security and achieve compliance to the AS17799 standard. A major advantage of using a fuzzy based approach, which became only evident midway through development, was that it allows for mapping inputs to different forms of confidence values. The general nature of fuzzy tables allows each question to be mapped in such a way so as the output of the fuzzy system represents the correct confidence factor. This single fact has been one of the most useful consequences in practical terms of developing the fuzzy based approach. It has saved a significant amount of time within government with the analysis of the security survey data.

With a fuzzy based approach, there is less importance on how the respondent values are saved in a database, as only the range of values is important. An expert uses the fuzzy tables to give definition to the values saved. The feature reduces the margin for error when developing surveys as the onus for value definition is now taken away from the programmer and becomes the complete responsibility of the survey expert. This is useful within the analysis stage as the coding for an on-line survey is done by a different set of people then those performing the analysis. The coders can use their own standard libraries and not have to worry about correct value mappings, and the experts now have more control over what those values actually mean. The result is a quicker setup time for the development of on-line surveys.

An independent review of 22 agencies progress towards obtaining their certification to AS/NZS17799.1:2001 was performed by the NSW Audit Office in 2004. The review was undertaken using a series of interviews rather than a formal survey. The audit report used three classifications of progress in their report (namely 'Limited Progress', 'Reasonable Progress' and 'Good Progress') which aligned closely with the same grouping in the results of the Fuzzy Logic study.

The further development of this project focuses on identifying the key issues and actions within successfully compliant agencies through the development of a fuzzy logic based on the structure of activity theory. If successful, the trained fuzzy logic will constitute a model for recognising agencies that could improve their existing information security in relation to the Australian standard.

6 IMPLICATIONS AND LIMITATIONS

A number of limitations have become apparent with the development of a fuzzy logic activity theory model. These are described as follows:

- The fuzzy logic model requires an expert to adjust the lookup tables. This involves some initial setup time.
- Time with regards to establishing confidence values for each question. This is also required when adding additional questions.
- The survey questions are answered by a number of people from different agencies. This introduces a human factor within the model, creating a potential for inconsistencies within the data set.

However, the fuzzy logic results provide an indicator of agency progress with the implementation of IS security standards compliance. The 2004 results were also independently verified by an outside agency. The fuzzy logic system was invaluable as a tool for data reduction to support management in problem-solving, planning, decision-making, saving time and resources.

7 CONCLUSION AND FUTURE DIRECTIONS

This paper studied e-Government use of fuzzy logic to measure or predict agencies gaining accreditation innovatively and it should be able to be applied not just across e-Government but across private organisations also (how well they are progressing to compliance with a standard). It is a measure of progress towards accreditation. The contribution to practice is the development of a fuzzy logic system grounded in IS theoretical methodology which facilitates the easy analysis of complex data in a dynamic context. The use of our approach also saves time being mostly an automated process from online survey input through expert interpretation of input parameters (weightings) to analysis outputted results. The results were a rank order or those government agencies ranging from highest rank and closest to independent compliance (accreditation imminent) to lowest ranked agencies where more resources are needed for them to be ready for the accreditation audit. Our results were verified by an independent auditor's study and found to be successful. Our methodology gives a global picture of an organisations move to accreditation i.e., a measure of IS security at a point in time. Future research directions include, continuing (longitudinal) research into the development and implementation of IS security policies, systems and measures in the government environment.

References

- Ammar, S., Moore, D., and Wright, R., (2008). Analysing customer satisfaction surveys using a fuzzy rule-based decision support system: Enhancing customer management. *Database Marketing & Customer Strategy Management*, 15(2), 91-105.
- Ammar, S., and Wright, R. (1995). A fuzzy logic approach to performance evaluation. *Proceedings of ISUMA-NAPIPS*, 246-251.
- Ammar, S., Wright, R., and Selden, S. (2000). Ranking state financial management: A multilevel fuzzy rule-based system. *Decision Science*, 31(2), Spring, 449-481.
- AS7799.2:2003. (2003). Information Security Management. Part 2. Specification for Information Security Management Systems, Standards Australia.
- Bannon, L. (1997). Activity Theory. www.sv.cict.fr/cotcos/pjs/TheoreticalApproaches
- Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25(4), December, 375-414.
- Clements, D. (1977). Fuzzy models for computer security system metrics. Unpublished Ph.D. thesis, University of California at Berkeley, Berkeley, California.
- Cox, E. (1994). *The Fuzzy Systems Handbook: A practitioner's guide to building, using, maintaining fuzzy systems*. Boston: AP Professional.
- Engeström, Y. (1987). Learning by expanding: An activity theoretical approach to development research. Helsinki Orienta-Konsultit.
- Engeström, Y. (1998). *Cultural-Historical Activity Theory*. Helsinki.
- Frank, D. (2003). Policy would secure users, transactions. *Federal Computer Week*, 17(2), 10.

Ghosh, S., Razouqi, Q., Schumacher, H. J., Celmins, A. (1998). A Survey of Recent Advances in Fuzzy Logic in Telecommunications Networks and New Challenges. *IEEE Transactions on Fuzzy Systems*, 6(3), August, 443-447.

Groves, S. (2003). The unlikely heroes of cyber security. *Information Management Journal*, May/June 37(3), 34.

Halpern, J. Y. (2003). Reasoning About Uncertainty. Cambridge, Mass: MIT Press.

Hasan, H., Gould E., Hyland P. (2001). Information Systems and Activity Theory: Tools in Context. University of Wollongong Press, Australia.

Hasan, H. (1999). Integrating IS and HCI using activity theory as a philosophical and theoretical basis. *Australasian Journal of Information Systems*, 6(2), May, 44-55.

Heeks, R.. (2002). eGovernment for development basic definitions page. IDPM, University of Manchester.

Hoffman, L., Michelman, E., Clements, D. (1998). SECURATE - security evaluation and analysis using fuzzy metrics. In *AFIPS National Computer Conference Proceedings 47*, AFIPS, Arlington, 531-540.

Hung, D., Nichani, M.R. (2002). Bringing communities of practice into schools: Implications for instructional technologies from vygotskian perspectives. *International Journal of Instructional Media*, 29(2), 171-183.

Klir, G. J. (1999). On fuzzy-set interpretation of possibility theory. *Fuzzy Sets and Systems*, 108, 263-273.

Nguyen, H. T. (2006). Fundamentals of Statistics with Fuzzy Data. Berlin Wu, Berlin: Springer.

Premiers Circular. "PC2001-46 Security of Electronic Information", (2001).

Rogers, Y. (2001). Knowledge transfer in a rapidly changing field: what can new theoretical approaches offer HCI? School of Cognitive and Computing Sciences, University of Sussex

Smith, S. (2006). Empirical Study of Information Systems Security Understanding and Awareness in E-Government. Unpublished PhD. Thesis, University of New South Wales.

Vrazalic, L. (2001). Techniques to analyse power and political issues in is development. In Information Systems and Activity Theory (Hasan H., Gould, E., Larkin, P. and Vrazalic, L. Eds), 2, *Theory and Practice*, 39-54, University of Wollongong.

Vygotsky, L. S. (1978). Mind in society: the development of higher psychological processes. Harvard University, Cambridge.

Zadeh, L. A. (1983). The role of fuzzy logic in the management of uncertainty in expert systems. *Fuzzy Sets and Systems*, 11, 199-227.